NAVAL WAR COLLEGE
Newport, RI

Information Warfare and the Principles of War

by

Anthony L. Scafidi

Major, USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy

Signature: Anthony L Scafidi

13 June 1997

Paper Directed by George W. Jackson, CAPT, USN
Chairman, Joint Military Operations Department

UNCLASSIFIED

Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Information Warfare and the Principles of War (unclassified)	
9. Personal Authors: Anthony L. Scafidi, Major, USAF	
10.Type of Report: FINAL	**11. Date of Report:** 7 Feb 1997
12.Page Count: 22	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Information Warfare, The Principles of War, Revolution in Military Affairs, 21st Century Warfare, Cypberspace, High-Tech, Command and Control Warfare, Hyper war, Information Dominance, C4I systems	

15.Abstract:

Within all the Services the debate is raging about information dominance, control of "cyberspace" or the "Infosphere" and Information Warfare. Some argue that Information Warfare (IW) is just a repackaging of old concepts and current practices, while others contend it is the next Revolution in Military Affairs (RMA). The question that needs to be addressed is; can IW achieve strategic and operational military objectives on its on merit? A way to answer this questions is to analyze IW against our current doctrine. Using the principles of war as a framework, does IW fit (or can it be employed) in the operational environment? Will it be necessary to redefine or update the principles of war to accommodate this changing environment?

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

Security Classification of This Page Unclassified

ABSTRACT

Within all the Services the debate is raging about information dominance, control of "cyberspace" or the "Infosphere" and Information Warfare. Some argue that Information Warfare (IW) is just a repackaging of old concepts and current practices, while others contend it is the next Revolution in Military Affairs (RMA). The question that needs to be addressed is: can IW achieve strategic and operational military objectives on its on merit? A way to answer this questions is to analyze IW against our current doctrine. Using the principles of war as a framework, does IW fit (or can it be employed) in the operational environment? Will it be necessary to redefine or update the principles of war to accommodate this changing environment?

Analyzing IW against the principles of war, illustrates that in most cases, the current definitions are valid and IW can be used to achieve operational objectives. Information technology and the increasing dependence on timely and accurate information is transforming the way we conduct business and is dramatically shaping the look of the 21st century battlefield. This transformation is shaping the way future wars will be fought and won. It would be naive to think that all wars in the future will be waged in the "Infosphere" alone. IW may not work in all situations, but the concepts can be selectively applied to assist with those operations. There is one thing, however, that will be true: as the dependency on information technology increases so too does our ability to exploit the opportunities it will create.

Table Of Contents

Information Warfare and the Principles of War

Are the Principles of War relevant in the face of Information Warfare?

"For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."
Sun Tzu[1]

Introduction

Within all the Services the debate is raging about information dominance, control of "cyberspace" or the "Infosphere" and Information Warfare. Some argue that Information Warfare is just a repackaging of old concepts and current practices, while others contend it is the next Revolution in Military Affairs (RMA).[2] In either case, warfare as we know it will change drastically in the 21st century. There is no argument that the need for and use of information has been going on since the beginning of war itself. The commander armed with superior battlefield information had a distinct advantage. The need and use of information, and dependence on information technologies in the current Information Age however, is expanding at a staggering rate.

In order to set the stage, it is important to establish a common reference or definition for the term Information Warfare (IW). The Joint Publications define IW as: "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer based networks."[3] Some of the readings would suggest that Command and Control Warfare (C2W) is the military application of IW. For the purposes of this paper, C2W will not be

addressed separately but will be included as a subset of IW. With that in mind, can IW achieve strategic and operational military objectives on its on merit? Are we moving toward the "bloodless" type of warfare (at least in the form of a reduction in American or Allied casualties) that Sun Tzu spoke of over 2000 years ago?

In order to answer these questions it is necessary to analyze IW against our current doctrine. Using the principles of war as a framework, does IW fit (or can it be employed) in the operational environment? In addition, given the potential for a possible Revolution in Military Affairs, will it be necessary to redefine or update the principles of war to accommodate this changing environment? It is a given that information dominance is a force multiplier. Without timely and accurate information, commanders can not make correct decisions. In addition, nations are becoming increasingly more dependent on information technology in every aspect of their existence. There are relatively few places left in the world where business is conducted with a stubby pencil. Also, developing nations are moving from agrarian societies directly into the "digital age." Information Warfare has the ability to capitalize on this dependency and exploit it to achieve our objectives. With that in mind, can IW stand on its own in the 21st century battlefield or is it just "another tool in the war-fighters' data base?"[4].

Information Warfare and the Principles of War

"The principles of war guide warfighting at the strategic, operational, and tactical levels. They are the enduring bedrock of US military doctrine."[5]

The above quote from Joint Pub 3-0 really sets the stage for the analysis of Information Warfare in today's environment. The principles of war have guided military commanders for years and are as enduring today in conventional warfare as they were in the past. With today's rapidly changing technology, can we achieve the same desired effects that have been possible by applying the tenets of the principles of war against a different form of warfare, one that downplays the use of "conventional" forces in favor of the "information-warrior"?

The Principle of Objective

Joint Pub 3-0 states that "the purpose of the objective is to direct every military operation towards a clearly defined, decisive, and attainable objective."[6] Of all the principles, having a clear objective is preeminent. In combat operations, the objective is to destroy the enemy forces' capabilities and will to fight. This is the cornerstone upon which all other principles build. Some would argue that IW is geared more toward achieving national strategic objectives and that Command and Control Warfare achieves objectives at the operational level.[7] However, as we move toward more technologically advanced adversaries and the electronic control of the battle space, IW techniques alone will be able to achieve

strategic, operational and most likely tactical objectives. In all likelihood it will be able to achieve these objectives, simultaneously.

The very nature of IW is geared toward attacking the enemy's decision-making processes. By changing the enemy's perception of the situation, you can make him believe he is in a no win situation. In addition, you can physically effect the information systems that control his weapon systems, defense system, logistics systems, transportation networks, financial institutions and utilities; either through manipulation of the data within these systems or through physical attacks. However, with IW it may now become unnecessary to physically destroy a target if you can render it useless through manipulation of the data within the system. Since we are concerned with the conditions in the country after hostilities have been terminated, it may be in our interest not to destroy their infrastructure. In addition, these internal attacks may remain imperceptible to the enemy for some time. He therefore thinks his systems are reliable and makes inaccurate decisions, possibly wasting additional manpower and resources. Taking out critical command and control functions, air defense systems, transportation networks and utilities can render the enemy defenseless and achieve our objectives. By targeting the enemy's information system we achieve our objectives while keeping our adversary from achieving his.[8]

The Principle of Offensive

The principle of war that is probably most appropriate to Information Warfare is offensive. US military doctrine defines offensive as the necessity to "seize, retain, and exploit the initiative" when engaged in combat operations.[9] The way an IW strategy would be implemented is focused on its offensive capabilities. The information warrior surreptitiously gains access to the enemy's information systems. He exploits these systems to gain as much intelligence as possible on the enemy's decision making process and capabilities. He then plants logic bombs, Trojan horses, or other such "devices" into the programs to await his command. At the time of his choosing, he springs these tools into action to seize the initiative.

Additionally, these attacks can be performed individually, sequentially or better yet, simultaneously. As Col John Warden, one of the architects of the air campaign in the 1991 Gulf War pointed out, future wars will feature parallel strikes aimed at all the key aspects of the adversary's war making capabilities. These parallel strikes are aimed at inflicting strategic paralysis and quick defeat and will occur simultaneously. His argument states that airpower will be the instrument of choice for such parallel or hyper-war. These simultaneous, parallel attacks are an excellent example of the need to gain and retain the offensive initiative.[10] By maintaining this high-level of activity, we also keep the enemy from having the chance to take to the offense. In today's environment, air power is probably the best choice in trying to achieve this form of hyper-war. In the 21st century, however, it will be possible to get these same results by

attacking the enemy's information systems and causing this same type of strategic paralysis.

The Principle of Mass

Throughout the history of warfare, the principle of mass has taken on different meanings. In the set-piece battles of Napoleonic times, it meant bringing as many troops to bear against the opponent as one could assemble. In its more recent iteration, it has taken on a somewhat different meaning. Joint Pub 3-0 defines the purpose of mass as the ability to "concentrate the *effects* [emphasis added] of combat power at the place and time to achieve decisive results."[11] IW has the ability to achieve mass by concentrating the effects of combat power against an adversary. In addition, through the ability to attack a multitude of targets, simultaneously, it may now be possible to achieve an even greater massing effect.

As illustrated in the Gulf War, the United States was able to use technology to achieve a high-tempo, parallel, and simultaneous operation that[12]

> overwhelmed the enemy's ability to respond. This advantage was built not only on advanced sensors and smart weapons, but perhaps more importantly on forces supported by modern C4I systems and technologies that allowed the United States to collapse previous spatial and temporal constraints . . . The number and tempo of these simultaneous parallel operations by themselves produced saturation effects that simply overloaded the enemy's command system. . .[13]

The use of IW techniques was thus able to achieve the effects of the principle of mass, by saturating the enemy's decision cycle. In the future, armed forces will be able to achieve the principle of mass (along with offensive), without having to resort to the assembly of large numbers of troops. Instead, they will saturate the enemy's decision systems and cause strategic paralysis.

The Principle of Economy of Force

The purpose of economy of force as defined in Joint Pub 3-0 is to "allocate minimum essential combat power to secondary efforts."[14] Basically, it is a recommendation to the military commander to concentrate most of his military power towards the primary threat rather than waste resources against a secondary task. In today's shrinking force structure, it is becoming increasing more difficult to support the two MRC concept. This decline in manpower and resources has made it paramount to find force multipliers to conduct our missions. In addition, we are being spread out even thinner by the need to support a multitude of Military Operation Other Than War.

The employment of IW technologies and techniques will provide the operational commander with the force multipliers necessary to achieve an "economy of force." In addition, it will now be possible to perform a multitude of faints and deceptions, using information technologies that will cause our adversary to violate his economy of force. "No longer will massive, dug-in armies fight bloody attritional battles. Instead small, highly mobile forces,

armed with real-time information from satellites and battlefield sensors, will strike with lightening speed in unexpected places. The winner: the side that can exploit information to disperse the fog of war, yet enshroud an enemy in it."[15] The principle of economy of force will still be valid in the face of IW, but will probably take on a different meaning.

The Principle of Maneuver/Movement

Historically, the concept of maneuver was meant to place or position your forces in relation to the enemy's fixed positions in order to gain or retain a geographical advantage. The Joint Pub states as the purpose "to place the enemy in a position of disadvantage through the flexible application of combat power."[16] Against the traditional understanding of the definition of the principle of maneuver, it would appear that IW can not position an adversary at a geographical disadvantage. However, in the literal sense, the flexible application of IW techniques can place the enemy at both a physical and psychological disadvantage. By blinding his command and control systems, it keeps him off balance. By manipulating or disabling his defensive systems, it increases our freedom of action and enables us to seize the initiative. In an article that appeared in *Time* magazine, Col Mike Tanksley described a possible scenario:

> First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Next, computer logic bombs, set to activate at

> predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, enemy field officers obey the orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert.[17]

In this way, the flexible application of IW's power has placed the enemy in a distinct position of disadvantage, possibly even stopping a war before it started.

The Principle of Unity of Command/Effort

Unity of Command is a principle of war that will take on a different meaning in the conduct of Information Warfare. Joint Pub 3-0 states: "ensure unity of effort under one responsible commander for every objective."[18] It goes without saying that for any type of warfare, you need one responsible individual who makes the ultimate decisions, and IW is no different. However, the explosion of information technologies has made it easier to provide rapid, real (and near-real) time command, control, communications, and intelligence (C3I). This capability will allow a more in-depth situational awareness of the enemy's forces and a greater control of our own.

The US Army in it's "Force XXI Operations" concept states that the advances in information technologies will create a horizontal integration of battlefield functions and assist commanders in tailoring their forces. There will be a wider dispersion of units, key nodes, and leaders. This will lead to the continuation of the empty battlefield phenomenon.[19] Of course, this type of

"digitally connected" command structure will not be unique to US or Allied forces alone. Our adversaries will most likely develop the same type of organizational structure. It is IW's ability to strike at this type of organization and disrupt the adversary's decision making cycle or Observe, Orient, Decide and Act (OODA) loop that makes it a perfect warfare strategy.[20] With the proper defensive IW strategy, we will be able to maintain our unity of command while totally destroying the enemy's. By causing him to violate another of his principles of war, we will achieve our objectives.

The Principle of Security

The principle of security is a key and essential part of defensive IW. This principle states that commanders should "never permit the enemy to acquire an unexpected advantage."[21] Further, the Joint Pub elaborates that having security enhances our freedom of action by reducing our vulnerability to hostile acts, influence or surprise. As we gain more and more dependence on information technology, it is imperative that we protect our decision making processes. We do not want the enemy to be able to affect our "OODA" loop while we are attacking his.

Of course one of the problems inherent with IW, is that it is really a "two-edged sword."[22] While you are connected to your adversaries computer system, he has access to your systems. Also, in order to be successful in an IW campaign you must have information superiority or dominance. The problem with

achieving information dominance is that it is not as easy to maintain in cyberspace. Achieving naval or air superiority keeps an enemy physically contained because there is a physical domain to control. By contrast, IW has no boundaries. And, as Martin Libicki points out: "Mastery of Information Warfare does not preclude an adversary from doing the same."[23] What makes matters worse is that an enemy does not have to be on an even parity or match our level of sophistication. A knowledgeable "hacker" with an old 286 IBM-compatible PC and a 2400 baud modem (probably bought at a yard sale for under $50) can do just as much damage as our best "info-warrior" armed with a Cray computer and the latest suite of high-speed digital communications.[24]

As we move into the next century, the capabilities of our adversaries will increase exponentially. Precisely how we will ensure the security of our information systems will continually change. But the underlying premise of this principle will not change only increase in importance.[25]

The Principle of Surprise

Coupled with the principle of offensive, surprise is another area where IW has a great potential. The purpose of surprise as defined by Joint Pub 3-0 is "to strike the enemy at a time or place or in a manner for which it is unprepared."[26] The tools of the information warrior: logic bombs, Trojan horses, viruses, clipped chips, sniffers, trap doors, worms and an ever increasing array of hardware and software techniques, are all based on the element of surprise. These tools and techniques are placed into the adversaries information and

decision making systems and remain dormant until they are needed. When needed, they can be activated to destroy a computer system, or to modify the data within the system. In some cases, the modification of the data, without the adversary knowing it has occurred, will be more devastating than the physical destruction of his facilities. Imagine the havoc that can be achieved by placing a program into an enemy's air defense network that adds a degree of altitude and azimuth to the firing solution computed by the targeting radar.[27] Or if the supply system was violated and every time a requisition for ammunition was placed into the system, the field site received ammonia. And the beauty of this situation is the enemy may not know this intrusion has occurred for weeks!

The Principle of Simplicity

Information technology will enhance the principle of simplicity as it is currently defined, but the definition might require some modification under the context of Information Warfare. Joint doctrine states the purpose as the need to "prepare clear, uncomplicated plans and concise orders to ensure thorough understanding."[28] Of course, in planning to conduct IW, it is essential that all plans and execution orders are clear, concise and directed toward the objective. However, the beauty of IW operations is in the simplicity of how they can be conducted. There is no need for massive amounts of logistics or transportation assets to move large numbers of troops. There are no boundaries or physical obstacles in cyberspace. IW can be conducted remotely, from the relative

security of protected facilities. In addition, our commanders will be connected through high speed digital networks (hopefully encrypted!), that will simplify our command and control process. "Modern technology allows the operational commander to collect, evaluate, analyze, and transmit information more quickly in the form of intelligence to higher and lower command echelons. C4I systems today allow the operational commander to communicate instantaneously with his forces, usually without interference."[29] This increased connectivity and access to real time intelligence will dramatically improve and enhance the principle of simplicity.

Conclusion

"What is called 'foreknowledge' cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation."
Sun Tzu[30]

Analyzing Information Warfare against the principles of war, illustrates that in most cases, the current definitions are valid and IW can be used to achieve operational objectives. IW can achieve surprise, seize the initiative, achieve the effects of mass, provide security (or violate the your enemy's security) and achieve objectives. IW will facilitate unity of command and provide the force multipliers necessary to achieve an economy of force. IW does not quite fit the current definitions for the principles of maneuver. IW can achieve the *effects* of maneuver and will place the enemy in a position of disadvantage. As for the principle of simplicity, we will still need to prepare clear and concise orders, but the idea of simplicity will probably take on a different meaning.

Information technology and the increasing dependence on timely and accurate information is transforming the way we conduct business and is dramatically shaping the look of the 21st century battlefield. This transformation is shaping the way future wars will be fought and won. It would be naive to think that all wars in the future will be waged in the "Infosphere" alone. IW may not work in all MOOTW situations, but the concepts can be selectively applied to assist with those operations. There is one thing, however

that will be true: as the dependency on information technology increases so too does our ability to exploit the opportunities it will create.

NOTES

[1] Sun Tzu, *Art of War* trans. Samuel B. Griffen (New York: Oxford University Press, 1963), p. 77.

[2] Alex Berger, "The Low Tech Side of Information Warfare," <(http://www.cdsar.af.mil/cc/berger.html>, (11 Jan 1997), p. 2.

[3] US Joint Chiefs of Staff, *Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W)* (Washington, DC. US Government Printing office, 7 February 1996), I-3.

[4] Norman B. Hutcherson, *Command & Control Warfare* (Maxwell AFB: 1994), cover page.

[5] US Joint Chiefs of Staff, *Joint Pub 3-0; Doctrine for Joint Operations* (Washington, DC; US Government Printing office, 1 February 1995), A-1.

[6] Joint Pub 3-0, A-1.

[7] Hutcherson, p. 17.

[8] US Air Force, *Cornerstones of Information Warfare* (Washington: 1995), <http://www.dtic.dla.mil/airforcelink/pubs/corner.html>, (14 December 1996), p. 1-9.

[9] Joint Pub 3-0, A-1

[10] John A. Warden III, *Air Theory for the Twenty-first Century*, in Karl P. Magyar, *Challenge and Response: Anticipating US Military Security Concerns*, (Maxwell AFB, Alabama: Air University Press August 1994), pp. 311-331.

[11] Joint Pub 3-0, A-1.

[12] Kenneth N. Firoved, "Is Mass Still a Valid Principle of War on Today's Battlefield?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 2 April 1996, p. 6.

[13] Jeffery R. Cooper, *Another View of the Revolution in Military Affairs* (Carlisle Barracks, PA: Strategic Studies Institute, 15 July 1994), p. 29-30.

[14] Joint Pub 3-0, A-1.

[15] John J. Arquilla and David F Ronfeldt, "Cyberwar and Netwar: New Modes, Old Concepts of Conflict" Excerpted from *Cyber War Is Coming*, by John J. Arquilla and David F. Ronfeldt, in Comparative Strategy, Vol. 12, pp. 141-165, 1993, <http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html>, (15 Dec 1996), p. 1.

[16] Joint Pub 3-0, A-2.

[17] Douglas W. Washington, "Onward Cyber Soldiers," *Time* Magazine, 21 August 1995, Vol 146, No. 8, <http://pathfinder.com/@@Q2PNVAQAY3j1HuGr/time/magazine/domestic/1995/950821/950821.cover.html >, (11 January 1997), p. 1.

[18] Joint Pub 3-0, A-2.

[19] US Army, Training and Doctrine Command (TRADOC), *Force XXI Operations: A Concept for the Evolution of Full-Dimension Operations for the Strategic Army of the Twenty-First Century*, TRADOC Pamphlet 525-5, August 1994, pp. 2-8.

[20] George A. Crawford, "Information Warfare: New Roles for Information Systems in Military Operations" <http://www.cdsar.af.mil/cc/crawford.html>, (11 Jan 1997), p. 2.

[21] Joint Pub 3-0, A-2.

[22] "Information Warfare: A Two-Edged Sword," (*Rand Research Review*, Fall, 1995), <http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html>, (10 December 1996), p. 1.

[23] Martin C. Libicki, "What Is Information Warfare?" *NDU Strategic Forum, Institute for National Strategic Studies* Number 28, May 1995, <http://www.ndu.edu/ndu/inss/strforum/forum28.html>, (13 December 96), p. 2.

[24] Stefan Eisen Jr., "Netwar, It's Not Just For Hackers Anymore," Unpublished Research Paper, US Naval War College, Newport, RI: 22 June 1995, p. 5.

[25] William T. Johnsen, et al., "The Principles of War In The 21ST Century: Strategic Considerations," 1 August 1995, <http://carlisle-www.army.mil/usassi/ssipubs/pubs95/pow21/pow21tc.htm>, (12 Jan 1997), p. 21.

[26] Joint Pub 3-0, A-2.

[27] Crawford, p. 6.

[28] Joint Pub 3-0, A-2.

[29] Milan N. Vego, "Operational Leadership," Unpublished Paper (NWC 4107) Naval War College, Newport, RI September 1996, p. 9.

[30] Sun Tzu, 145.

Bibliography

Arquilla, John J. and Ronfeldt, David F. "Cyberwar and Netwar: New Modes, Old Concepts of Conflict" Excerpted from *Cyber War Is Coming*, by John J. Arquilla and David F. Ronfeldt, in Comparative Strategy, Vol. 12, pp. 141-165, 1993. <http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html>. (15 Dec 1996).

Berger, Alex. "The Low Tech Side of Information Warfare." Air University Air Chronicles, CADRE's On-Line. <http://www.cdsar.af.mil/cc/berger.html>. (11 Jan 1997).

Campen, Alan D. *First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf*, Farfax, VA. (AFCEA International Press, 1992).

Cardwell, Thomas A. III. *Command Structure for Theater Warfare: The Quest for Unity of Command.* Maxwell AFB, AL. (Air University Press, September 1984).

Cooper, Jeffery R., *Another View of the Revolution in Military Affairs* (Carlisle Barracks, PA: Strategic Studies Institute, 15 July 1994).

Crawford, George A. "Information Warfare: New Roles for Information Systems in Military Operations." Air University Air Chronicles, CADRE's On-Line. <http://www.cdsar.af.mil/cc/crawford.html>, (11 Jan 1997).

Eisen, Stefan Jr., "Netwar, It's Not Just For Hackers Anymore." Unpublished Research Paper, US Naval War College, Newport, RI. 22 June 1995.

Firoved, Kenneth N. "Is Mass Still a Valid Principle of War on Today's Battlefield?" Unpublished Research Paper. U.S. Naval War College, Newport, RI. 2 April 1996

Gompert, David C. "Keeping Information Warfare in Perspective." <http://www.rand.org/publications/RRR/RRR.fall95.cyber/perspective.html>. (11 Jan 1997).

Hutcherson, Norman B. *Command and Control Warfare. Putting Another Tool in the War-Fighter's Data Base.* Maxwell AFB, AL: (Air University Press, September 1994).

"Information Warfare: A Two-Edged Sword." (*Rand Research Review*, Fall, 1995).
<http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html>. (10 December 1996).

Johnsen, William T., et al. "The Principles of War In The 21ST Century: Strategic Considerations." 1 August 1995. <http://carlisle-www.army.mil/usassi/ssipubs/pubs95/pow21/pow21tc.htm>. (12 Jan 1997).

Konopatzke, Kurt. "Information Warfare: Same wine, different bottle?" Air University Air Chronicles, CADRE's On-Line.
<http://www.cdsar.af.mil/cc/iw2.html>. (10 December 1996).

Kuehl, Dan. "The Ethics of Information Warfare and Statecraft." NDU/School of Information Warfare & Strategy.
<http://www.infowar.com/mil_c4i/mil_c4i.html-ssi>. (15 December 1996).

Libicki, Martin C. "What Is Information Warfare?" *NDU Strategic Forum, Institute for National Strategic Studies* Number 28, May 1995, <http://www.ndu.edu/ndu/inss/strforum/forum28.html>. (13 December 96).

Marr, Patrick M. "Information Warfare and the Operational Art" Unpublished Research Paper. U.S. Naval War College, Newport, RI. 12 February 1996

Munro, Neil. "A Look At The On-Line Frontier The Pentagon's New Nightmare: An Electronic Pearl Harbor." *Washington Post.* 16 July 1995. (http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html). (15 December 1996).

Orr, George E. *Combat Operations C3I: Fundamentals and Interactions.* Maxwell AFB, Al. (Air University Press, July 1983).

Snyder, Frank M. *Command and Control. The Literature and Commentaries.* Washington, DC. (National Defense University Press. September 1993).

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Super Highway.* (New York: Thunder's Mouth Press, 1994).

Sun Tzu, *Art of War* trans. Samuel B. Griffen (New York: Oxford University Press, 1963).

Szafranski, Richard. "A Theory of Information Warfare." Air University Air Chronicles, CADRE's On-Line. <http://www.cdsar.af.mil/apj/szfran.html>. (11 Jan 1997).

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the Twenty-First Century.* (Boston, Little, Brown, 1993)

US Air Force, "Cornerstones of Information Warfare." (Washington: 1995). <http://www.dtic.dla.mil/airforcelink/pubs/corner.html>. (14 December 1996)

US Air Force Fact Sheet 95-20. "Information Warfare." November 1995. <http://www.dtic.dla.mil/airforcelink/pa/factsheets/information_warfare.html>. (14 December 1996).

US Army, Training and Doctrine Command (TRADOC), *Force XXI Operations: A Concept for the Evolution of Full-Dimension Operations for the Strategic Army of the Twenty-First Century*, TRADOC Pamphlet 525-5, August 1994.

US Joint Chiefs of Staff, *Joint Pub 3-0; Doctrine for Joint Operations* (Washington, DC; US Government Printing Office, 1 February 1995).

US Joint Chiefs of Staff, *Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W)* (Washington, DC; US Government Printing Office, 7 February 1996).

Van Creveld, Martin. *Technology and War From 2000 B.C. to the Present.* (New York: The Free Press, 1989).

Vego, Milan N., "Operational Leadership", Unpublished Paper (NWC 4107) Naval War College, Newport, RI. September 1996.

Warden, John A. III, *Air Theory for the Twenty-first Century*, in Magyar, Karl P. *Challenge and Response: Anticipating US Military Security Concerns.* Maxwell AFB, Al. (Air University Press August 1994).

Washington, Douglas W. "Onward Cyber Soldiers," *Time Magazine*, 21 August 1995, Vol. 146, No. 8. <http://pathfinder.com/@@Q2PNVAQAY3j1HuGr/time/magazine/domestic/1995/950821/950821.cover.html>, (11 January 1997).

Winnefield, James A. and Johnson, Dana J. *Joint Air Operations: Pursuit of Unity in Command and Control, 1942-1991.* Annapolis, MD. (Naval Institute Press, 1993).